Report – Projeto #include

Gabriela Centrone Canella

São Paulo
13 de junho de 2021

Introdução

Como parte da entrega final do projeto de extensão #include, foi necessário realizarmos um report das vulnerabilidades encontradas em nosso aplicativo desenvolvido. Utilizando o teste de penetração básico do OWASP ZAP, obteve-se os resultados abaixo identificados.

Resultados obtidos

- CSP: Wildcard Directive

As seguintes diretivas permitem fontes curinga (ou ancestrais), não são definidas ou são definidas de forma ampla: quadro-ancestrais, forma-ação.
A(s) diretiva(s): frame-ancestors, form-action estão entre as diretivas que não retrocedem para default-src, perdê-las/excluí-las é o mesmo que permitir qualquer coisa.

Solução: Certifique-se de que seu servidor web, servidor de aplicativos, balanceador de carga, esteja configurado corretamente para definir o cabeçalho Content-Security-Policy.

- Cross-Domain Misconfiguration

O carregamento de dados do navegador da web pode ser possível, devido a uma configuração incorreta do Cross Origin Resource Sharing (CORS) no servidor da web.

Solução: Certifique-se de que os dados confidenciais não estejam disponíveis de maneira não autenticada (usando a lista branca de endereços IP, por exemplo).
Configure o cabeçalho HTTP "Access-Control-Allow-Origin" para um conjunto mais restritivo de domínios ou remova todos os cabeçalhos CORS inteiramente, para permitir que o navegador da web aplique a Same Origin Policy (SOP) de uma maneira mais restritiva.

- X-Frame-Options Header Not Set

O cabeçalho X-Frame-Options não está incluído na resposta HTTP para proteção contra ataques de 'ClickJacking'.

Solução: A maioria dos navegadores da Web modernos oferece suporte ao cabeçalho HTTP X-Frame-Options. Certifique-se de que está definido em todas as páginas da web retornadas por seu site (se você espera que a página seja enquadrada apenas por páginas em seu servidor (por exemplo, é parte de um FRAMESET), então você vai querer usar SAMEORIGIN, caso contrário, se você nunca espera a página para ser enquadrado, você deve usar DENY. Como alternativa, considere a implementação da diretiva "frame-ancestors" da Política de segurança de conteúdo.

- Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

O servidor da web/aplicativo está vazando informações por meio de um ou mais cabeçalhos de resposta HTTP "X-Powered-By". O acesso a essas informações pode facilitar que os invasores identifiquem outras estruturas/componentes dos quais seu

aplicativo da web depende e as vulnerabilidades às quais esses componentes podem estar sujeitos.

Solução: Certifique-se de que seu servidor web, servidor de aplicativos, balanceador de carga, etc. esteja configurado para suprimir cabeçalhos "X-Powered-By".

- X-Content-Type-Options Header Missing

O cabeçalho X-Content-Type-Options do Anti-MIME-Sniffing não foi definido como 'nosniff'. Isso permite que versões mais antigas do Internet Explorer e do Chrome executem a detecção de MIME no corpo da resposta, potencialmente fazendo com que o corpo da resposta seja interpretado e exibido como um tipo de conteúdo diferente do tipo de conteúdo declarado. As versões atuais (início de 2014) e legadas do Firefox usarão o tipo de conteúdo declarado (se houver), em vez de realizar a detecção de MIME.

Solução: Certifique-se de que o aplicativo/servidor da web defina o cabeçalho Content-Type apropriadamente e que defina o cabeçalho X-Content-Type-Options como 'nosniff' para todas as páginas da web.
Se possível, certifique-se de que o usuário final use um navegador da web moderno e compatível com os padrões que não execute a detecção de MIME ou que possa ser direcionado pelo aplicativo / servidor da web para não executar a detecção de MIME.

- Information Disclosure - Suspicious Comments

A resposta parece conter comentários suspeitos que podem ajudar um invasor. Nota: As correspondências feitas em blocos de script ou arquivos são em relação a todo o conteúdo, não apenas aos comentários.

Solução: Remova todos os comentários que retornam informações que podem ajudar um invasor e corrigir quaisquer problemas subjacentes aos quais eles se referem.

- Timestamp Disclosure – Unix

Um timestamp foi divulgado pelo aplicativo/servidor web – Unix.

Solução: Confirme manualmente se os dados do carimbo de data/hora não são confidenciais e se os dados não podem ser agregados para divulgar padrões exploráveis.